UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

529 Glenwood Avenue, Apt 1, Cincinnati, Ohio 45229

Case No. 1:24-MJ-729

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	Certain Activities Relating to material involving the sexual exploitation of minors
18 U.S.C. § 2252A	Certain activities relating to material constituting or containing child pornography

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Ryan R Snyder

Applicant's signature

Ryan Snyder, Special Agent FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime *(specify reliable electronic means)*.

Date: Sep 13, 2024

Stephanie K. Bowman

Judge's signature

City and state: Cincinnati, Ohio

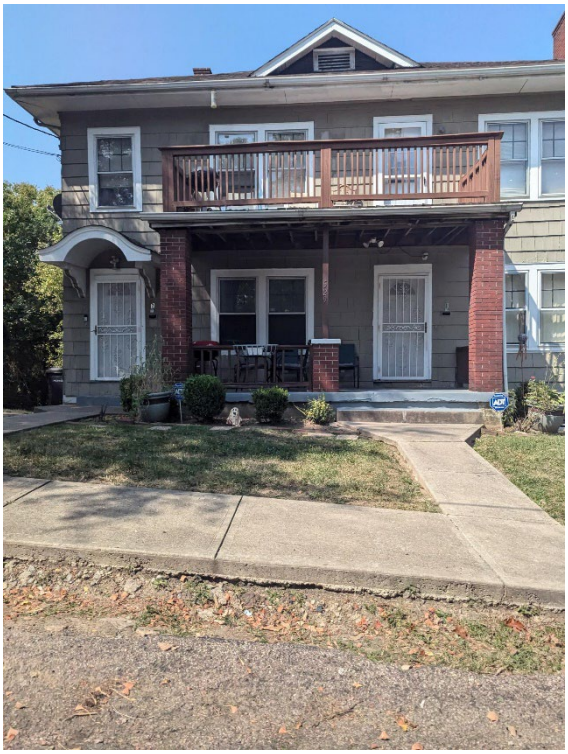
Stephanie K. Bowman, United States Magistrate Judge

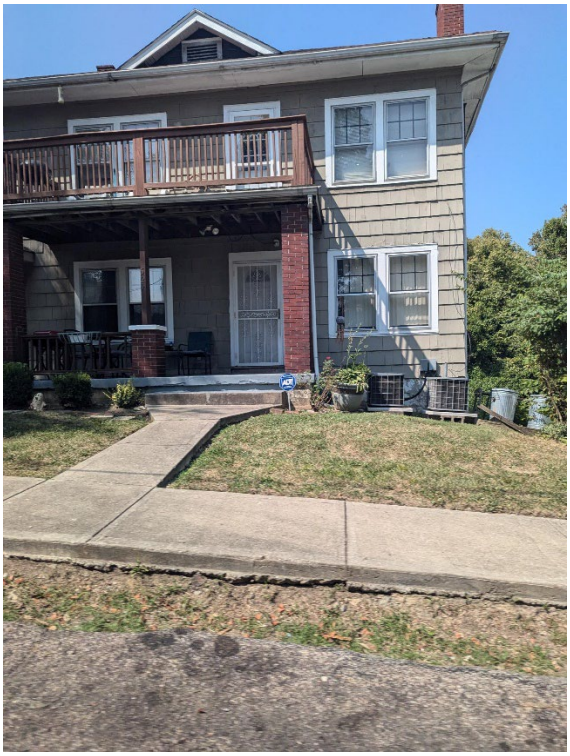
Printed name and title

ATTACHMENT A1

Property to Be Searched

529 Glenwood Avenue, Apartment 1, Cincinnati, Ohio 45229 is a two-story duplex style residence with olive colored siding and a red-brown roof. The building is divided into apartments number one (1) and two (2). The residence in question is Apartment 1. The driveway is located on the south side of the home. When looking at the building from Glenwood Avenue, apartment one is located on the viewer right (north) side and apartment two is located on the viewer left (south) side. There is a concrete walkway leading to the front door. There is a two-story deck style porch attached to the home. The entrance to apartment one is under the deck.





ATTACHMENT B LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), including cell phones, computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica; and the contents therein.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. Any and all visual depictions of minors, in any format and medium, including all originals, computer files, copies, and negatives, engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer at the residence located at 529 Glenwood Avenue, Apartment 1, Cincinnati, Ohio 45229 by use of the computer

or by other means for the purpose of distributing or receiving visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern any accounts with an Internet Service Provider.

7. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Any and all diaries, notebooks, notes, and any other records reflecting a person's sexual interest in minors. Any and all diaries, notebooks, notes, and any other records reflecting personal contact or any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF the residence located at 529 Glenwood Avenue, Apt 1, Cincinnati, Ohio 45229 and 216 East 9th Street, Unit# 404, Cincinnati, Ohio 45202.	Case No. 1:24-MJ-729 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ryan R. Snyder, a special agent with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the residence located at 529 Glenwood Avenue, Apartment 1, Cincinnati, Ohio (OH) 45229 (hereafter referred to as location/attachment A1) and 216 East 9th Street, Unit# 404, Cincinnati, Ohio 45202 (hereafter referred to as location/attachment A2) . The information to be searched is described in the following paragraphs and in Attachment B. This affidavit is made in support of an application for a search warrant.

2. I have been employed as a Special Agent with the FBI since 2024 and am currently assigned to the Cincinnati Joint Terrorism Task Force. I was assigned to assist the violent crimes squad in FBI Cincinnati headquarters office with a child pornography case. Prior to joining the FBI I served as a municipal police officer from January 2017 through January 2024. In my position I am responsible for investigating violations of law involving various violent crimes to include crimes against children.

3. During my career as a law enforcement officer, I participated in various investigations involving computer-related offenses and executed 50+ search warrants to include

those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a special agent, I investigate criminal violations relating to child exploitation and child pornography including the illegal distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

4. As a special agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. Along with other agents and officers of the Federal Bureau of Investigation and other law enforcement agencies, I am currently involved in an investigation of the sharing and distribution of child pornography by JAYLIN ILER, in addition to others as yet unidentified. This Affidavit is submitted in support of a search warrant for the main subject current residence as described in Attachment A1 and his former residence as described in attachment A2.

6. As part of the investigation, I reviewed documentation and reports provided by and discussed information with other officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that JAYLIN ILER distributed child pornography in violation

of 18 U.S.C. § 2252 and 18 U.S.C. §§ 2252A. There is also probable cause to search the residence described in Attachment A for evidence of these crimes, as described in Attachment B.

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, including cellphones, and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers, including cell phones, basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to anyone of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks - such as engaging in online chat, sharing digital files, reading a book, or playing a game - on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child

pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

g. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that mobile device users often connect to known wireless networks which are available to them, especially localized networks within their residence. The connection information such as usernames and passwords are typically stored within the device and the device automatically connects when within range of a known wireless network. Individuals often set this automatic connect preference in their devices in order to conserve battery consumption, improve connection speeds, and reduce cellular data consumption which is often limited or metered. Mobile devices connected to a wireless network will often share the same IP address information as reported by the residential wireless network provider.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

10. The storage capacity of the electronic storage media used in home computers and cell phones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. A user can set up an online storage account from any computer or cell phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or cell phone. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or cell phone in most cases.

12. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files.

13. Social media and messenger applications, such as Telegram, SnapChat, Facebook, and X as well as others, are used by those with an interest in child pornographic material to send, receive, and store files containing child pornography. Additionally, these applications are used to have discussions related to sexual interest in children with others online.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

14. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

15. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

16. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

17. Child pornography collectors often reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a

community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

18. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, to include Internet cloud storage. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

19. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

PROBABLE CAUSE

20. On May 15, 2024 West Chester Police Department (WCPD) received a walk in complaint to their police station regarding the distribution of child pornography. The

complaining witness (herein after "CW") exchanged Facebook Messenger messages with JAYLIN ILER from May 3, 2024 through May 16, 2024. In the course of their conversations ILER sent the CW a photograph of an approximately 13-15 year old, naked, black male with an erect penis. The following conversation took place.

CW: "Lol wasi [sic] supposed to get this"

ILER: "Yea lol [two face emojis]"

CW: "Lol he look young"

ILER: "[Face emoji] he is lol"

21. On the evening of May 15, 2024 ILER sent the cooperating witness ten (10) Facebook Messenger messages which the CW received overnight. Prior to the CW reviewing the messages, ILER recalled or "unsent" the messages which deleted them from the CW's view. The CW asked ILER what the messages contained. ILER sent the CW additional images that depicted underage males in various states of undress. One image showed a naked, 13-14 year old black male laying curled up on a bed, exposing his buttocks to the camera. Another photo depicted a teenage black male, naked from the waist down, leaning over a bed, exposing his buttock to the camera.

22. The CW asked ILER if the young boys were sending the messages to him (ILER) directly. ILER responded no. The images came from an online group where such images were shared.

23. After initially messaging using the Facebook Messenger application, ILER invited the CW to join the application known as Telegram. I know that Telegram is a cellphone communication and media sharing application frequently used to exchange content such as child pornography. Telegram is end to end encrypted which limits law enforcement's ability to access

application content. Content is privatized and cannot be access by legal process because Telegram is hosted outside of the United States, does not respond to U.S. legal process, and given the encrypted nature of the application, the host company is unable to view content of private groups and messages.

24. CW entered the application at ILER's request. ILER invited the CW to a Telegram group known as "Black NL Gay Teens!". Once inside the group the CW viewed a large quantity of child pornography being exchanged. The images varied from juveniles in various states of undress to images of infants being penetrated by adults males by use of the adults penis and fingers.

25. The CW captured screenshots of his messages with ILER as well as the images ILER sent in Facebook Messenger. THE CW saved the screenshots to later show law enforcement. The CW went to the WCPD and presented the facts of this case as well as the screenshots he captured. WCPD determined it did not have jurisdiction over the incident and referred the matter to the FBI for follow up.

26. I know that Facebook accounts can be referenced by either their account number or an associated vanity URL. The Facebook accounts in question for this incident are vanity user name JvDaicon (CW's account) and 61558805573595 (ILER's account). On May 16, 2024 a preservation request for both accounts was submitted by WCPD as part of their initial investigation and accepted by Facebook.

27. On August 20, 2024 I received records for ILER and the CW's Facebook accounts pursuant to a search warrant served on Facebook's parent company, Meta Inc. Review of the records revealed several items of interest that support this investigation and application.

28. ILER'S Facebook contained several images of child pornography. The images included photos of a naked, 13-15 year old black male standing in front of a mirror. The male was taking a photo of himself holding his erect penis in his hand. Another image showed the same male with his arm raised above his head so that his erect penis was exposed to the camera.

29. I also located a Facebook Messenger conversation between ILER and another male who is not related or involved in this investigation beyond the described Facebook chat with ILER. In their conversation ILER sent the male a short video showing a 13-15 year old black male dancing with his buttocks exposed to the camera. Several other juveniles are observed in the background. The uninvolved male commented to ILER that the people seen in the video are kids. ILER responded by saying they are "almost grown".

30. I also reviewed the content of the CW's Facebook account. As described above in paragraph 10 of this affidavit, when ILER and the CW messaged in real time, ILER deleted his portion of the conversation as well as the images he sent the CW. In the CW's Facebook record return I was able to recover the full, undeleted Facebook Messenger exchange between ILER and the CW as well as the photos ILER sent.

31. ILER sent the CW numerous images of child pornography. The images showed a 13-15 year old black male standing in front of a mirror. The male took several photos of himself in various states of undress. In several images the male was completely naked standing in front of the mirror. The male had an erect penis. In some photos he held his penis in his hands, in others he stood with his arm above his head exposing his penis. Several photos showed the same male in front of a mirror with his pants pulled down to expose his buttocks to the camera.

32. The CW asked ILER where he got photos of the young male. ILER responded and the following exchange took place.

ILER: "CP group im Finna stop watching this shit tho."

ILER: "It's on telegram."

PEGG: "Whats that lol?"

ILER: "Child prn."

33. I know based on my training and experience that "CP" refers to child pornography.

34. ILER then invited the CW to a Telegram channel that allows member to share child pornography. Prior to the CW entering the Telegram channel, ILER told the CW to "brace" himself because there may be some things in the Telegram group the CW is not "into".

35. On August 31, 2024 a second cooperating witness (CW2) walked into the Cincinnati Police Department and reported ILER shared child pornography with him via Facebook Messenger. CW2 reported that ILER sent CW2 a message claiming that he (ILER) was in a group of adults involved in unspecified "inappropriate" activities with toddlers.

36. ILER sent CW2 two images showing naked, black toddlers in various compromising positions. One showed an adult black male spreading a child's buttocks with his hands. The other showed a naked black toddler.

37. I also received two tips submitted to the National Center for Missing and Exploited Children (NCMEC) that involved ILER. NCMEC is a national clearing house for child pornography reports from internet service providers. Internet service providers (ISP) like Facebook that locate child pornography on their platforms, report the images and/or conversation to NCMEC which intakes the complaint. NCMEC compiles and reviews the child pornography images and information about the account holder then forwards the complaint to the appropriate law enforcement agency for follow up.

38. NCMEC forwarded two independent complaints from separate ISPs that identified ILER as the account holder of accounts which posted or shared child pornography.

39. X (formerly Twitter) reported three images and/or messages that were associated with X username "Coochiebumper69". The account was registered to email address jayiler3@icloud.com and cellular telephone number (513) 646-5551. Legal process returns revealed that the email and phone number were registered to Jaylin Iler of location A1.

40. I reviewed the complaint and found two specific images X reported. The images were the same and showed an infant laying face down on a blanket. A white male inserted his erect penis into the infant's anus. The third flagged item was a file containing the media content of ILER's X account. I reviewed the content of the files and observed numerous images that were obviously child pornography. One such image showed a black adult male licking a black infant female's vagina.

41. X also flagged a tweet that contained the following message. "Who wants the video of this one year old boy getting fucked?"

42. I reviewed the second NCMEC tip which was submitted by the ISP SnapChat. SnapChat is an image sharing and messaging platform. Users can send one another messages directly as well as post messages, videos and status updates for all users to see.

43. The SnapChat account that was flagged and reported to NCMEC was for user Jaypretty08. The user registered his account with email address Jayiler08@gmail.com and provided a date of birth in 1996. Legal process returns for Jayiler08@gmail.com showed the account owner to be Jay Iler. The date of birth provided by SnapChat matched ILER's date of birth.

44. I reviewed the image flagged and provided by SnapChat. It showed a screenshot of a naked, adult, black male holding a naked, black, infant female with her leg spread exposing her vagina to the camera.

45. I know from my training and experience that SnapChat and X are social media platforms that are available for use in both a web-based and application-based platform. Web based access can be made from any system that has connection to the internet. This includes computers, tablets, or cellphones. The application-based access can be made from any platform that can download the specific ISPs application. Based on my training and experience I know that the most common systems for downloading and accessing ISP applications are tablets and cell phones.

SPECIFICS OF THE REQUEST FOR TWO SEARCH WARRANTS

46. Through all of my investigation to this point, ILER resided at location A1. On Wednesday September 12, 2024 I learned that ILER was arrested for domestic assault against another occupant of location A1. Upon his release from jail, ILER was excluded from the residence and barred from returning to the home.

47. ILER was placed on electronic monitoring by the Hamilton County Adult Probation Department. ILER provided a new residence to his probation officer. That new residence was location A2 where he resides with a family member. With the exception of three, four-hour, court authorized windows, ILER is restricted to location A2. His probation officer can view near real time data that shows ILER's location.

48. Based on tracking data ILER did not return to location A1 following his arrest and has complied with his probation requirements. Based on my training and experience, it is unlikely that ILER was able to retrieve any computers or other electronic devices beyond what

was on his person at the time of arrest. Those items he was unable to retrieve likely remain at location A1.

49. I also know that individuals generally do not travel without access to their cellphones or other communication devices. Following ILER's release from jail and occupancy of location A2, it is probable that he retained his cellphone.

50. I also know that individuals, particularly persons who view and share child pornography keep the computer or cellphone the store images on nearby, so they have ready access to the images. Because ILER is now residing at location A2, his cellphone and thus evidence of child pornography are probably in his possession at the new residence.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

51. As described above and in Attachment B, this application seeks permission to search for records that might be found at the premises, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

52. I submit that if a computer or storage medium is found at the premises, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

53. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate

how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to advertise, distribute, transport, receive, possess, or access child pornography, or to act in furtherance of any conspiracy to take these acts, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit

a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

54. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or

intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

55. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though

wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

56. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

USE OF BIOMETRIC FEATURES TO UNLOCK DEVICES

57. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or

facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of

the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with

biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual present during the execution of the warrant to the fingerprint scanner of the device; (2) hold the device in front of the face of any individual present during the execution of the warrant to activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. The premises warrant for the property described in Attachments A1 and A2 will be searched by law enforcement officers for the items described in B.

CONCLUSION

59. Based on the foregoing, I request that the Court issue the proposed search warrants.

REQUEST FOR SEALING

60. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Ryan R Snyder

Ryan R. Snyder
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September 13, 2024 via FaceTime

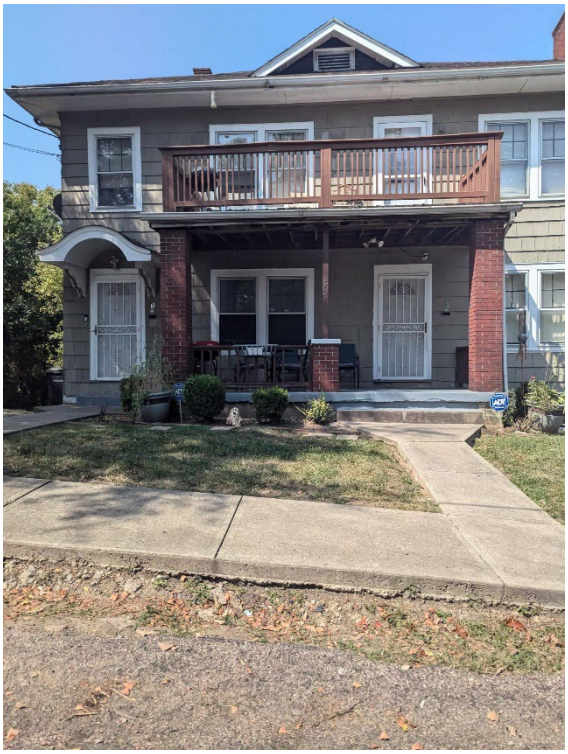
Stephanie K. Bowman

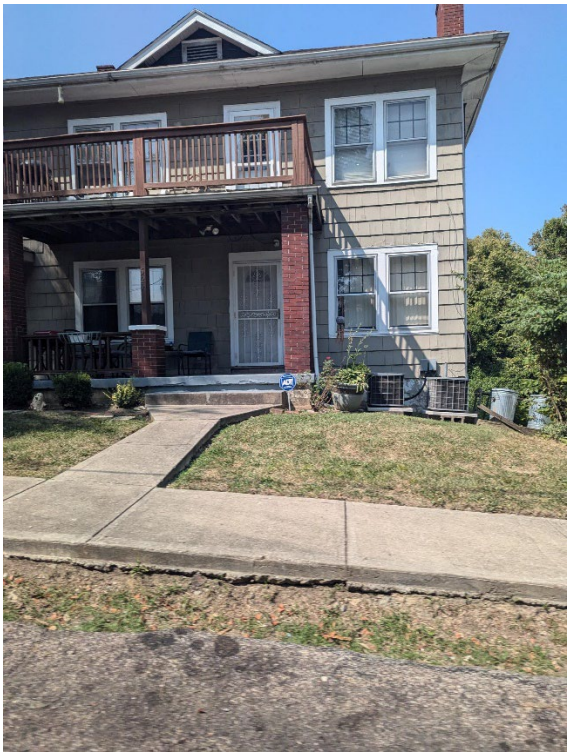
STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1

Property to Be Searched

529 Glenwood Avenue, Apartment 1, Cincinnati, Ohio 45229 is a two-story duplex style residence with olive colored siding and a red-brown roof. The building is divided into apartments number one (1) and two (2). The residence in question is Apartment 1. The driveway is located on the south side of the home. When looking at the building from Glenwood Avenue, apartment one is located on the viewer right (north) side and apartment two is located on the viewer left (south) side. There is a concrete walkway leading to the front door. There is a two-story deck style porch attached to the home. The entrance to apartment one is under the deck.





ATTACHMENT B LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), including cell phones, computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica; and the contents therein.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. Any and all visual depictions of minors, in any format and medium, including all originals, computer files, copies, and negatives, engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer at the residence located at 529 Glenwood Avenue, Apartment 1, Cincinnati, Ohio 45229 by use of the computer

or by other means for the purpose of distributing or receiving visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern any accounts with an Internet Service Provider.

7. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Any and all diaries, notebooks, notes, and any other records reflecting a person's sexual interest in minors. Any and all diaries, notebooks, notes, and any other records reflecting personal contact or any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).